Statement of

J. Brent Williams

Chief Technology Officer, Anakam, Inc.

before the

Health Information Technology Standards Committee

Privacy and Security Workgroup

Panel: Building Trust

November 19, 2009

Statement of J. Brent Williams

Chief Technology Officer

Anakam, Inc.

HIT Standards Committee Privacy and Security Workgroup

Building Trust Panel

November 19, 2009

Dr. Baker and members of the workgroup, thank you for the opportunity to share our thoughts on building trust within the health information technology community today. My name is Brent Williams, and I am the Chief Technology Officer of Anakam. Anakam provides software that establishes trusted identities for very large scale user populations through our standards-based approach to progressive multi-factor authentication and the associated identity proofing and verification. In my role as the CTO, I work with our existing and prospective customers, largely in the healthcare, government, banking, and education markets, to identify the next generation of changes required in our product to satisfy emerging needs and requirements. At the same time, I work across all of our customers to provide best practice recommendations for the incorporation of trusted identity and access solutions within their environment and the transformational impact on their business.

While the healthcare industry is unique in its terminology, the business relationships between stakeholders, and the particular sensitivity of data, the challenge of establishing trust within the electronic healthcare community is remarkably similar to challenges in other industries and the federal government. In the end, we all seek a safe way that very sensitive information can be stored, moved, and presented such that it is only revealed to those who need to know it; we seek solutions that make sure our information will not be altered intentionally or unintentionally; and, finally, we need the information when we ask for it. These same trust concepts exist where paper medical records are still used, but the risks are not as great as they are easier to control.

While the comprehensive view of trust is critical, my remarks will focus on the way identity plays a role in establishing trust. Many of the core elements of security used to establish trust around networks, systems, and applications have been discussed and reviewed with exhaustive depth. Alternatively, while identity plays a role in security of each of these, identity is

fundamental to trust in health information systems at a level abstracted above these core security elements. While username and password can log a person into an application, or a token or proximity badge can get somebody access to a server, this still does not provide a comprehensive view of identity across the enterprise. The comprehensive view of identity across the enterprise takes several key elements into consideration. First, identity manages two forms of risk. The first is granting access to sensitive information. The second is establishing non-repudiation. Identity risk associated with access control is exemplified by a patient accessing self-entered PHR data where the risk is that the person accessing the data is not the same person who entered it. Non-repudiatory risk is exemplified by e-prescribing solutions wherein liability can be associated with incorrect actions, and therefore knowing who conducted the transaction is as important as what the transaction contained. Another element that drives an enterprise view is the fact that the role of individuals within the electronic healthcare enterprise is dynamic. A person that is one day a practitioner will also be a patient. The identity remains the same, but the role is dynamic; without an enterprise view of identity, it would be difficult to provide appropriate rights to each role.

The electronic health enterprise is evolving to keep up with the rest of the commercial marketplace. There are two potential routes the healthcare marketplace will adopt. Barring regulatory challenges to its success in the healthcare market, cloud-based computing, wherein data and applications are no longer the dominion of the desktop and the server but instead reside anywhere in the network, creates a whole new set of challenges around data protection and identity. EHR and PHR data may be stored in the "cloud", e-prescribing and telemedicine may become cloud-based services, in which case the security of the underlying infrastructure will be lost. Where cloud-based computing cannot succeed, the concept that allows data to rest where it was created is an alternative. Even in this scenario, data will be accessible by the broader user base provided they have the proper authorization to get to the information as systems are more and more networked. Identity is at the crux of both of these potential outcomes. No matter which path we go down in electronic healthcare, or even if we choose a hybrid of both, to provide security and trust, there must exist a unique tie between the person accessing the data and the data itself. Patients will give digital consent of their trust to share information with another practitioner, and practitioners will have access to all of the records and information they have created or been given consent to have access.

Identity has a lifecycle. An identity is created, it is updated and changed, and it is eventually abandoned. Despite our best efforts, the identity lifecycle is not an absolute process. It follows the basic tenets of risk management – even as a basic face-to-face transaction, we cannot guarantee that the person presenting themselves for a transaction is who they claim. We can ask for more government identification, ask a lot of questions, check out their background, and search the "databases". In the end, we make a measured risk decision that this is good enough.

The process has a few key steps. A person presents themselves to register; once they provide their biographic information, we then need to confirm that information through identity proofing and verification. If the person asserts professional credentials that will afford them certain privileges, these credentials need to be verified. At this point, the person is assigned credentials that represent their identity. These could be as simple as an identity badge for physical access controls or a username and password as well as a token for logical access controls. As it relates to electronic systems, they use these electronic credentials to authentication to systems such that their asserted identity can be verified. Once verified, the electronic identity is given access to the enterprise applications to which it is authorized. As the role of the identity evolves (such as intern becomes doctor) or changes temporally (such as a practitioner becomes a patient) the person may be authorized access to additional or fewer applications or information. The elemental steps are registration, identity proofing, professional credentialing, authentication, authorization, access control, and change management.

A person with a higher level of responsibility and access should go through a stronger series of identity lifecycle steps whereas a person with lesser responsibility and access could undergo less rigorous identity verification. To manage risk appropriately, the principle of the "weakest link in the chain" should be followed. The strength of the identity is established by the weakest process step in establishing the identity. So, if a person is put in a role of substantial trust and access, and consequently has detailed identity verification and proofing, but only weak username and password requirements, the trust threshold lies with the weak username and password. Conversely, for usability sake, if a person with low level access has to jump through numerous hoops, the value of these steps is limited, the cost is higher, and the likelihood that they will follow the process is low. Consequently, identity management practices and risk management practices should be directly aligned.

Business practices around identity are changing too. As risk management justifies the need for stronger identity verification for some, and lesser for others, the practices of medicine are evolving. The practitioner can no longer provider their credentials to a few key people in the office so those people can perform their transactions for them. Alternatively, everybody will have an identity and a role, the load will be removed from the practitioner by shifting the business process. For example, current e-prescribing practices leads practitioners to share their usernames and passwords with nurses or administrators in their office. The practitioners take on the non-repudiatory risk as they have trusted their office staff to conduct some of those transactions. As we seek to shift to the electronic prescription of controlled substances, these higher strength credentials prevent the sharing or multiple use of the credential. A practitioner will respond that this will increase their workload and responsibility because they cannot offload by sharing their credentials. Alternatively, our work in this space shows

transformational business processes wherein practitioners still take ultimate responsibility through their authentication transaction to “sign” the prescription, but the workflow can be offloaded from the practitioner by assigning roles in the prescribing process that allow others to prepare the script and associated charting, but the practitioner releases it with their “signature”. With this modified workflow, not only do you have the ability to assign non-repudiation to the practitioner – a key element to controlled substances e-prescribing – but all key members of the electronic healthcare workflow process will have risk-adjusted authentication transactions establishing similar non-repudiation instead of using the practitioner’s credentials.

In conclusion, while there are many components of establishing trust in the electronic healthcare environment, an enterprise view of how identities are established, registered, authenticated, and managed is an essential component to establishing trust within the evolving electronic healthcare enterprise. Furthermore, many of these strategies are independent of the form and direction of electronic healthcare in the near future. I sincerely appreciate the opportunity to provide our remarks, and I look forward to the questions you may have.